

# WEIGHT ENUMERATOR OF SOME IRREDUCIBLE CYCLIC CODES

F. E. BROCHERO MARTÍNEZ AND C. R. GIRALDO VERGARA

**ABSTRACT.** In this article, we show explicitly all possible weight enumerators for every irreducible cyclic code of length  $n$  over a finite field  $\mathbb{F}_q$ , in the case which each prime divisor of  $n$  is also a divisor of  $q - 1$ .

## 1. INTRODUCTION

A code of length  $n$  and dimension  $k$  over a finite field  $\mathbb{F}_q$  is a linear  $k$ -dimensional subspace of  $\mathbb{F}_q^n$ . A  $[q; n, k]$ -code  $\mathcal{C}$  is called *cyclic* if it is invariant by the shift permutation, i.e., if  $(a_1, a_2, \dots, a_n) \in \mathcal{C}$  then the shift  $(a_n, a_1, \dots, a_{n-1})$  is also in  $\mathcal{C}$ . The cyclic code  $\mathcal{C}$  can be viewed as an ideal in the group algebra  $\mathbb{F}_q C_n$ , where  $C_n$  is the cyclic group of order  $n$ . We note that  $\mathbb{F}_q C_n$  is isomorphic to  $\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$  and since subspaces of  $\mathcal{R}_n$  are ideals and  $\mathcal{R}_n$  is a principal ideal domain, it follows that each ideal is generated by a polynomial  $g(x) \in \mathcal{R}_n$ , where  $g$  is a divisor of  $x^n - 1$ .

Codes generated by a polynomial of the form  $\frac{x^n - 1}{g(x)}$ , where  $g$  is an irreducible factor of  $x^n - 1$ , are called *minimal cyclic codes*. Thus, each minimal cyclic code is associated of natural form with an irreducible factor of  $x^n - 1$  in  $\mathbb{F}_q[x]$ . An example of minimal cyclic code is the Golay code that was used on the Mariner Jupiter-Saturn Mission (see [6]), the BCH code used in communication systems like VOIP telephones and Reed-Solomon code used in two-dimensional bar codes and storage systems like compact disc players, DVDs, disk drives, etc (see [5, Section 5.8 and 5.9]). The advantage of the cyclic codes, with respect to other linear codes, is that they have efficient encoding and decoding algorithms (see [5, Section 3.7]).

For each element of  $g \in \mathcal{R}_n$ ,  $\omega(g)$  is defined as the number of non-zero coefficient of  $g$  and is called the *Hamming weight of the word  $g$* . Denote by  $A_j$  the number of codewords with weight  $j$  and by  $d = \min\{i > 0 | A_i \neq 0\}$  the minimal distance of the code. A  $[q; n, k]$ -code with minimal distance  $d$  will be denoted by  $[q; n, k, d]$ -code. The sequence  $\{A_i\}_{i=0}^n$  is called the *weight distribution* of the code and  $A(z) := \sum_{i=0}^n A_i z^i$  is its *weight enumerator*. The importance of the weight distribution is that it allows us to measure the probability of non-detecting an error of the code: For instance, the probability of undetecting an error in a binary symmetric channel is  $\sum_{i=0}^n A_i p^i (1-p)^{n-i}$ , where  $p$  is the probability that, when the transmitter sends a binary symbol (0 or 1), the receptor gets the wrong symbol.

---

*Date:* May 12, 2014.

*2010 Mathematics Subject Classification.* 12E05(primary) and 94B05(secondary).

*Key words and phrases.* Cyclic Codes, Weight Enumerator, minimal distance.

The weight distribution of irreducible cyclic codes has been determined for a small number of special cases. For a survey about this subject see [3], [4] and their references.

In this article, we show all the possible weight distributions of length  $n$  over a finite field  $\mathbb{F}_q$  in the case which every prime divisor of  $n$  divides  $q - 1$ .

## 2. PRELIMINARIES

Throughout this article,  $\mathbb{F}_q$  denotes a finite field of order  $q$ , where  $q$  is a power of a prime,  $n$  is a positive integer such that  $\gcd(n, q) = 1$ ,  $\theta$  is a generator of the cyclic group  $\mathbb{F}_q^*$  and  $\alpha$  is a generator of the cyclic group  $\mathbb{F}_{q^2}^*$  such that  $\alpha^{q+1} = \theta$ . For each  $a \in \mathbb{F}_q^*$ ,  $\text{ord}_q a$  denotes the minimal positive integer  $k$  such that  $a^k = 1$ , for each prime  $p$  and each integer  $m$ ,  $\nu_p(m)$  denotes the maximal power of  $p$  that divides  $m$  and  $\text{rad}(m)$  denotes the radical of  $m$ , i.e., if  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$  is the factorization of  $m$  in prime factors, then  $\text{rad}(m) = p_1 p_2 \cdots p_l$ . Finally,  $a_{\div b}$  denotes the integer  $\frac{a}{\gcd(a, b)}$ .

Since each irreducible factor of  $x^n - 1 \in \mathbb{F}_q[x]$  generates an irreducible cyclic code of length  $n$ , then a fundamental problem of code theory is to characterize these irreducible factors. The problem of finding a “generic algorithm” to split  $x^n - 1$  in  $\mathbb{F}_q[x]$ , for any  $n$  and  $q$ , is an open one and only some particular cases are known. Since  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ , where  $\Phi_d(x)$  denotes the  $d$ -th cyclotomic polynomial (see [7] theorem 2.45), it follows that the factorization of  $x^n - 1$  strongly depends on the factorization of the cyclotomic polynomial that has been studied by several authors (see [9], [8], [11] and [2]).

In particular, a natural question is to find conditions in order to have all the irreducible factors binomials or trinomials. In this direction, some results are the following ones

**Lemma 2.1.** [1, Corollary 3.2] *Suppose that*

- (1)  $\text{rad}(n)|(q - 1)$  and
- (2)  $8 \nmid n$  or  $q \not\equiv 3 \pmod{4}$ .

*Then the factorization of  $x^n - 1$  in irreducible factors of  $\mathbb{F}_q[x]$  is*

$$\prod_{t|m} \prod_{\substack{1 \leq u \leq \gcd(n, q-1) \\ \gcd(u, t)=1}} (x^t - \theta^{ul}),$$

*where  $m = n_{\div (q-1)}$  and  $l = (q - 1)_{\div n}$ . In addition, for each  $t$  such that  $t|m$ , the number of irreducible factors of degree  $t$  is  $\frac{\varphi(t)}{t} \cdot \gcd(n, q - 1)$ , where  $\varphi$  denotes the Euler Totient function.*

**Lemma 2.2.** [1, Corollary 3.4] *Suppose that*

- (1)  $\text{rad}(n)|(q - 1)$  and
- (2)  $8 \mid n$  and  $q \equiv 3 \pmod{4}$ .

*Then the factorization of  $x^n - 1$  in irreducible factors of  $\mathbb{F}_q[x]$  is*

$$\prod_{\substack{t|m' \\ t \text{ odd}}} \prod_{\substack{1 \leq w \leq \gcd(n, q-1) \\ \gcd(w, t)=1}} (x^t - \theta^{wl}) \cdot \prod_{t|m'} \prod_{u \in S_t} (x^{2t} - (\alpha^{ul'} + \alpha^{qu l'})x^t + \theta^{ul'}),$$

where  $m' = n_{\div (q^2-1)}$  and  $l = (q-1)_{\div n}$ ,  $l' = (q^2-1)_{\div n}$ ,  $r = \min\{\nu_2(\frac{n}{2}), \nu_2(q+1)\}$  and  $\mathcal{S}_t$  is the set

$$\left\{ u \in \mathbb{N} \left| \begin{array}{l} 1 \leq u \leq \gcd(n, q^2-1), \gcd(u, t) = 1 \\ 2^r \nmid u \text{ and } u < \{qu\}_{\gcd(n, q^2-1)} \end{array} \right. \right\},$$

where  $\{a\}_b$  denotes the remainder of the division of  $a$  by  $b$ , i.e. it is the number  $0 \leq c < b$  such that  $a \equiv c \pmod{b}$ .

In addition, for each  $t$  odd such that  $t|m'$ , the number of irreducible binomials of degree  $t$  and  $2t$  is  $\frac{\varphi(t)}{t} \cdot \gcd(n, q-1)$  and  $\frac{\varphi(t)}{2t} \cdot \gcd(n, q-1)$  respectively, and the number irreducible trinomials of degree  $2t$  is

$$\begin{cases} \frac{\varphi(t)}{t} \cdot 2^{r-1} \gcd(n, q-1), & \text{if } t \text{ is even} \\ \frac{\varphi(t)}{t} \cdot (2^{r-1} - 1) \gcd(n, q-1), & \text{if } t \text{ is odd.} \end{cases}$$

### 3. WEIGHT DISTRIBUTION

Throughout this section, we assume that  $\text{rad}(n)$  divides  $q-1$  and  $m, m', l, l'$  and  $r$  are as in the lemmas 2.1 and 2.2. The following results characterize all the possible cyclic codes of length  $n$  over  $\mathbb{F}_q$  and show explicitly the weight distribution in each case.

**Theorem 3.1.** *If  $8 \nmid n$  or  $q \not\equiv 3 \pmod{4}$ , then every irreducible code of length  $n$  over  $\mathbb{F}_q$  is a  $[q; n, t, \frac{n}{t}]$ -code where  $t$  divides  $m$  and its weight enumerator is*

$$A(z) = \sum_{j=0}^t \binom{t}{j} (q-1)^j z^{j\frac{n}{t}} = (1 + (q-1)z^{\frac{n}{t}})^t.$$

*Proof:* As a consequence of Lemma 2.1, every irreducible factor of  $x^n - 1$  is of the form  $x^t - a$  where  $t|n$  and  $a^{n/t} = 1$ , so every irreducible code  $\mathcal{C}$  of length  $n$  is generated by a polynomial of the form

$$g(x) = \frac{x^n - 1}{x^t - a} = \sum_{j=0}^{n/t-1} a^{\frac{n}{t}-1-j} x^{tj}$$

and  $\{g(x), xg(x), \dots, x^{\frac{n}{t}-1}g(x)\}$  is a base of the  $\mathbb{F}_q$ -linear subspace  $\mathcal{C}$ . Thus, every codeword in  $\mathcal{C}$  is of the form  $a_0g + a_1xg + \dots + a_{t-1}x^{t-1}g$ , with  $a_j \in \mathbb{F}_q$ , and

$$\omega(a_0g + a_1xg + \dots + a_{t-1}x^{t-1}g) = \omega(a_0g) + \omega(a_1xg) + \dots + \omega(a_{t-1}x^{t-1}g).$$

Since  $\omega(g) = \frac{n}{t}$ , it follows that

$$\omega(a_0g + a_1xg + \dots + a_{t-1}x^{t-1}g) = \frac{n}{t} \#\{j | a_j \neq 0\}.$$

Clearly we have  $A_k = 0$  for all  $k$  that is not divisible by  $\frac{n}{t}$ . On the other hand, if  $k = j\frac{n}{t}$ , then exactly  $j$  elements of this base have non-zero coefficients in the linear combination and each non-zero coefficient can be chosen of  $q-1$  distinct forms, hence  $A_k = \binom{t}{j}(q-1)^j$ . Then the weight distribution is

$$A_k = \begin{cases} 0, & \text{if } t \nmid k \\ \binom{t}{j}(q-1)^j, & \text{if } k = j\frac{n}{t} \end{cases}$$

as we want to prove.  $\square$

**Remark 3.2.** *The previous result generalizes Theorem 3 in [10] (see also Theorem 22 in [4]).*

**Remark 3.3.** *As a direct consequence of Lemma 2.1, for all  $t$  positive divisor of  $m$ , there exist  $\frac{\varphi(t)}{t} \gcd(n, q-1)$  irreducible cyclic  $[q; n, t, \frac{n}{t}]$ -codes.*

In order to find the weight distribution in the case which  $q \equiv 3 \pmod{4}$  and  $8|n$ , we need some additional lemmas.

**Lemma 3.4.** *Let  $t$  be a positive integer such that  $t$  divides  $m'$  and assume that  $q \equiv 3 \pmod{4}$ . If  $x^{2t} - (a + a^q)x^t + a^{q+1} \in \mathbb{F}_q[x]$  is an irreducible trinomial, where  $a = \alpha^{ul'} \in \mathbb{F}_{q^2}$ , and  $g(x)$  is the polynomial  $\frac{x^n - 1}{x^{2t} - (a + a^q)x^t + a^{q+1}} \in \mathbb{F}_q[x]$ , then  $\nu_2(u) \leq r - 2$  and*

$$\omega(g(x) - \lambda x^t g(x)) = \begin{cases} \frac{n}{t} \left(1 - \frac{1}{2^{r-\nu_2(u)}}\right), & \text{if } \lambda \in \Lambda_u \\ \frac{n}{t}, & \text{if } \lambda \notin \Lambda_u, \end{cases}$$

$$\text{where } \Lambda_u = \left\{ \frac{a^i - a^{qi}}{a^{i+1} - a^{q(i+1)}} \mid i = 0, 1, \dots, 2^{r-\nu_2(u)} - 2 \right\}.$$

*Proof:* Since  $x^{2t} - (a + a^q)x^t + a^{q+1}$  is an irreducible trinomial in  $\mathbb{F}_q[x]$ , then  $\gcd(t, u) = 1$ ,  $2^r \nmid u$  and  $a \neq -a^q$ . In particular,  $\text{ord}_{q^2} a$  does not divide either  $q-1$  or  $2(q-1)$ . Observe that

$$\begin{aligned} \text{ord}_{q^2} a &= \frac{q^2 - 1}{\gcd(q^2 - 1, ul')} \\ &= \frac{q^2 - 1}{\gcd\left(q^2 - 1, u \frac{q^2 - 1}{\gcd(q^2 - 1, n)}\right)} \\ &= \frac{\gcd(q^2 - 1, n)}{\gcd(q^2 - 1, n, u)} \\ &= \frac{2^r \gcd(q - 1, n)}{\gcd(2^r(q - 1), n, u)}, \end{aligned}$$

and for each odd prime  $p$ , we have

$$\nu_p\left(\frac{2^r \gcd(q - 1, n)}{\gcd(2^r(q - 1), n, u)}\right) \leq \nu_p(\gcd(q - 1, n)) \leq \nu_p(q - 1). \quad (3.1)$$

Therefore

$$\nu_2\left(\frac{2^r \gcd(q - 1, n)}{\gcd(2^r(q - 1), n, u)}\right) = r + 1 - \nu_2(u) > \nu_2(2(p - 1)) = 2. \quad (3.2)$$

On the other hand

$$\begin{aligned} g(x) &= \frac{x^n - 1}{x^{2t} - (a + a^q)x^t + a^{q+1}} \\ &= \frac{x^n - 1}{a - a^q} \left( \frac{1}{x^t - a} - \frac{1}{x^t - a^q} \right) \\ &= \sum_{j=1}^{n/t-1} \left( \frac{a^j - a^{qj}}{a - a^q} \right) x^{n-t-tj}, \end{aligned}$$

is a polynomial whose degree is  $n - 2t$  and every non-null monomial is such that its degree is divisible by  $t$ . Now, suppose that there exist  $1 \leq i < j \leq \frac{n}{t} - 2$  such that the coefficients of the monomials  $x^{n-t-jt}$  and  $x^{n-t-it}$  in the polynomial  $g_\lambda := g(x) - \lambda x^t g(x)$  are simultaneously zero. Then

$$\frac{a^j - a^{qj}}{a - a^q} = \lambda \frac{a^{j+1} - a^{q(j+1)}}{a - a^q} \quad \text{and} \quad \frac{a^i - a^{qi}}{a - a^q} = \lambda \frac{a^{i+1} - a^{q(i+1)}}{a - a^q}.$$

So, in the case which  $\lambda \neq 0$ , we have

$$\lambda = \frac{a^j - a^{qj}}{a^{j+1} - a^{q(j+1)}} = \frac{a^i - a^{qi}}{a^{i+1} - a^{q(i+1)}}.$$

This last equality is equivalent to  $a^{(q-1)(j-i)} = 1$ , i.e.,  $\text{ord}_{q^2} a$  divides  $(q-1)(j-i)$ . In the case  $\lambda = 0$ , we obtain that  $\text{ord}_{q^2} a$  divides  $(q-1)j$  and  $(q-1)i$  by the same argument. Thereby, we can treat this case as a particular case of the above one making  $i = 0$ . It follows that  $\frac{2^r \gcd(q-1, n)}{\gcd(2^r(q-1), n, u)}$  divides  $(q-1)(j-i)$ .

So, by the Equation (3.1), the condition  $\text{ord}_{q^2} a | (q-1)(j-i)$  is equivalent to

$$\nu_2 \left( \frac{2^r \gcd(q-1, n)}{\gcd(2^r(q-1), n, u)} \right) = r + 1 - \nu_2(u) \leq \nu_2((p-1)(j-i)) = 1 + \nu_2(j-i),$$

and therefore  $2^{r-\nu_2(u)} | (j-i)$ .

In other words, if the coefficient of the monomial of degree  $n - t - it$  is zero, then all the coefficients of the monomials of degree  $n - t - jt$  with  $j \equiv i \pmod{2^{r-\nu_2(u)}}$  are zero. Thus, if  $\lambda \notin \Lambda_u$ , then any coefficient of the form  $x^{tj}$  is zero and the weight of  $g_\lambda$  is  $\frac{n}{t}$ . Otherwise, exactly  $\frac{n}{t} \cdot \frac{1}{2^{r-\nu_2(u)}}$  coefficients of the monomials of the form  $x^{tj}$  are zero, then the weight of  $g_\lambda$  is  $\frac{n}{t} \left(1 - \frac{1}{2^{r-\nu_2(u)}}\right)$ , as we want to prove.  $\square$

**Corollary 3.5.** *Let  $g$  be a polynomial in the same condition of lemma 3.4. Then*

$$\# \left\{ (\mu, \lambda) \in \mathbb{F}_q^2 \mid \omega(\mu g(x) + \lambda x^t g(x)) = \frac{n}{t} \left(1 - \frac{1}{2^{r-\nu_2(u)}}\right) \right\} = 2^{r-\nu_2(u)}(q-1).$$

*Proof:* If  $\mu = 0$  and  $\lambda \neq 0$ , then  $\omega(\lambda x^t g(x)) = \frac{n}{t} \left(1 - \frac{1}{2^{r-\nu_2(u)}}\right)$  and we have  $(q-1)$  ways to choose  $\lambda$ .

Suppose that  $\mu \neq 0$ , then  $\omega(\mu g(x) + \lambda x^t g(x)) = \omega\left(g(x) + \frac{\lambda}{\mu} x^t g(x)\right)$ , i.e. the weight only depends on the quotient  $\frac{\lambda}{\mu}$ . By Lemma 3.4 there exist  $2^{r-\nu_2(u)} - 1$  values of  $\frac{\lambda}{\mu}$  such that  $g(x) + \frac{\lambda}{\mu} x^t g(x)$  has weight  $\frac{n}{t} \left(1 - \frac{1}{2^{r-\nu_2(u)}}\right)$ , so we have  $(q-1)(2^{r-\nu_2(u)} - 1)$  pairs of this type.  $\square$

**Theorem 3.6.** *If  $8|n$  and  $q \equiv 3 \pmod{4}$ , then every irreducible code of length  $n$  over  $\mathbb{F}_q$  is one of the following class:*

(a) A  $[q; n, t, \frac{n}{t}]$ -code, where  $4 \nmid t$ ,  $t|m'$  and its weight enumerator is

$$A(z) = \sum_{j=0}^t \binom{t}{j} (q-1)^j z^{j \frac{n}{t}} = (1 + (q-1)z^{\frac{n}{t}})^t.$$

(b) A  $[q; n, 2t, d]$ -code, where  $t|m'$ ,  $d = \frac{n}{t} \left(1 - \frac{1}{2^{r-\nu_2(u)}}\right)$ ,  $0 \leq u \leq r-2$  and its weight enumerator is

$$A(z) = \left(1 + 2^{r-\nu_2(u)}(q-1)z^d + (q-1)(q+1-2^{r-\nu_2(u)})z^{\frac{n}{t}}\right)^t.$$

In particular, if  $\frac{n}{t 2^{r-\nu_2(u)}} \nmid k$ , then  $A_k = 0$ .

*Proof:* Observe that every irreducible code is generated by a polynomial of the form  $\frac{x^n-1}{x^t-a}$  where  $a \in \mathbb{F}_q$ , or a polynomial of the form  $g(x) = \frac{x^n-1}{(x^t-a)(x^t-a^q)}$ , where  $a$  satisfies the condition of lemma 3.4. In the first case, the result is the same of the Theorem 3.1. In the second case, each codeword is of the form

$$\sum_{j=0}^{2t-1} \lambda_j x^j g(x) = \sum_{j=0}^{t-1} h_j,$$

where  $h_j = \lambda_j x^j g(x) + \lambda_{t+j} x^{t+j} g(x)$ . Since, for  $0 \leq i < j \leq t-1$ , the polynomial  $h_i$  and  $h_j$  do not have non-null monomials of the same degree, it follows that

$$\omega \left( \sum_{j=0}^{t-1} h_j \right) = \sum_{j=0}^{t-1} \omega(h_j).$$

By Lemma 3.4,  $h_j$  has weight  $\frac{n}{t}$ ,  $d$  or 0, for all  $j = 0, \dots, t-1$ . For each  $j = 0, 1, \dots, t-1$ , there exist  $(q^2-1)$  non-null pairs  $(\lambda_j, \lambda_{j+t})$ , and by Corollary 3.5, we know that there exist  $2^{r-\nu_2(u)}(q-1)$  pairs with weight  $d$ . Therefore, there exist

$$q^2 - 1 - 2^{r-\nu_2(u)}(q-1) = (q-1)(q+1 - 2^{r-\nu_2(u)})$$

pairs with weight  $\frac{n}{t}$ .

So, in order to calculate  $A_k$ , we need to select which  $h_i$ 's have weight  $d = \frac{n}{t}(1 - \frac{1}{2^{r-\nu_2(u)}})$  and which ones have weight  $\frac{n}{t}$ , so that the total weight is  $k$ .

If we chose  $i$  of the first type and  $j$  of the second type, the first  $h_i$ 's can be chosen by  $\binom{t}{i} (2^{r-\nu_2(u)}(q-1))^i$  ways and for the other  $t-i$  ones, there are  $\binom{t-i}{j} ((q-1)(q+1 - 2^{r-\nu_2(u)}))^j$  ways of choosing  $j$  with weight  $\frac{n}{t}$ . The remaining  $h_j$ 's have weight zero. Therefore

$$A_k = \sum_{\substack{k=di+\frac{n}{t}j \\ 0 \leq i+j \leq t}} \binom{t}{i} \left( 2^{r-\nu_2(u)}(q-1) \right)^i \binom{t-i}{j} \left( (q-1)(q+1 - 2^{r-\nu_2(u)}) \right)^j,$$

and

$$\begin{aligned} A(z) &= \sum_{0 \leq i+j \leq t} \binom{t}{i,j} \left( 2^{r-\nu_2(u)}(q-1)z^d \right)^i \left( (q+1 - 2^{r-\nu_2(u)})(q-1)z^{\frac{n}{t}} \right)^j \\ &= \left( 1 + 2^{r-\nu_2(u)}(q-1)z^d + (q-1)(q+1 - 2^{r-\nu_2(u)})z^{\frac{n}{t}} \right)^t. \end{aligned}$$

In particular, the minimal distance is  $d$  and every non-null weight is divisible by  $\gcd(d, \frac{n}{t}) = \frac{n}{t2^{r-\nu_2(u)}}$ .  $\square$

**Remark 3.7.** As a direct consequence of Lemma 2.2, for all  $t$  positive divisor of  $m'$ , there exist  $2^{r-1-\nu_2(u)} \frac{\varphi(t)}{t} \gcd(n, q-1)$  irreducible cyclic  $[q; n, t, d]$ -codes if  $t$  is odd, and  $2^{r-1} \frac{\varphi(t)}{t} \gcd(n, q-1)$  irreducible cyclic  $[q; n, 2t, \frac{n}{t}(1 - \frac{1}{2^r})]$ -codes if  $t$  is even.

**Example 3.8.** Let  $q = 31$  and  $n = 288 = 2^5 \times 3$ . Then  $m' = 3$ ,  $l' = 10$ ,  $r = 4$ . If  $h(x)$  denotes a irreducible factor of  $x^{288} - 1$ , then  $h(x)$  is a binomial of degree 1, 2, 3 or 6, or a trinomial of degree 2 or 6. The irreducible codes generated by  $\frac{x^n-1}{h(x)}$  (and therefore parity check polynomial  $h$ ), and its weight enumerators are showed in the following tables

| CODES GENERATED BY BINOMIALS   |            |                     |
|--------------------------------|------------|---------------------|
| $[q; n, t, \frac{n}{t}]$ -Code | $h(x)$     | Weight enumerator   |
| [31; 288, 1, 288]              | $x + 1$    | $1 + 30z^{288}$     |
|                                | $x + 5$    |                     |
|                                | $x + 6$    |                     |
|                                | $x + 25$   |                     |
|                                | $x + 26$   |                     |
|                                | $x + 30$   |                     |
|                                | $x^2 + 1$  |                     |
|                                | $x^2 + 5$  |                     |
|                                | $x^2 + 25$ |                     |
| [31; 288, 2, 144]              | $x^3 + 5$  | $(1 + 30z^{144})^2$ |
|                                | $x^3 + 6$  |                     |
|                                | $x^3 + 25$ |                     |
|                                | $x^3 + 26$ |                     |
| [31; 288, 3, 96]               | $x^6 + 5$  | $(1 + 30z^{96})^3$  |
|                                | $x^6 + 25$ |                     |
| [31; 288, 6, 48]               | $x^6 + 5$  | $(1 + 30z^{48})^6$  |
|                                | $x^6 + 25$ |                     |

| CODES GENERATED BY TRINOMIALS OF THE FORM $x^2 + ax + b$ |            |                  |                               |
|--|------------|------------------|-------------------------------|
| $[q; n, 2t, d]$ -Code                                    | $\nu_2(u)$ | $h(x)$           | Weight enumerator             |
| [31; 288, 2, 216]  | 2          | $x^2 + 8x + 1$   | $1 + 120z^{216} + 840z^{288}$ |
|  |            | $x^2 + 9x + 25$  |                               |
|  |            | $x^2 + 14x + 5$  |                               |
|  |            | $x^2 + 17x + 5$  |                               |
|  |            | $x^2 + 22x + 25$ |                               |
|  |            | $x^2 + 23x + 1$  |                               |
| [31; 288, 2, 252]  | 1          | $x^2 + x + 5$    | $1 + 240z^{252} + 720z^{288}$ |
|  |            | $x^2 + 5x + 1$   |                               |
|  |            | $x^2 + 6x + 25$  |                               |
|  |            | $x^2 + 8x + 25$  |                               |
|  |            | $x^2 + 9x + 5$   |                               |
|  |            | $x^2 + 14x + 1$  |                               |
|  |            | $x^2 + 17x + 1$  |                               |
|  |            | $x^2 + 22x + 5$  |                               |
|  |            | $x^2 + 23x + 25$ |                               |
|  |            | $x^2 + 25x + 25$ |                               |
|  |            | $x^2 + 26x + 1$  |                               |
|  |            | $x^2 + 30x + 5$  |                               |
| [31; 288, 2, 270]  | 0          | $x^2 + 2x + 5$   | $1 + 480z^{270} + 480z^{288}$ |
|  |            | $x^2 + 4x + 1$   |                               |
|  |            | $x^2 + 4x + 5$   |                               |
|  |            | $x^2 + 7x + 5$   |                               |
|  |            | $x^2 + 7x + 25$  |                               |
|  |            | $x^2 + 8x + 5$   |                               |
|  |            | $x^2 + 9x + 1$   |                               |
|  |            | $x^2 + 10x + 1$  |                               |
|  |            | $x^2 + 11x + 1$  |                               |
|  |            | $x^2 + 11x + 25$ |                               |
|  |            | $x^2 + 12x + 25$ |                               |
|  |            | $x^2 + 14x + 25$ |                               |
|  |            | $x^2 + 17x + 25$ |                               |
|  |            | $x^2 + 19x + 25$ |                               |
|  |            | $x^2 + 20x + 1$  |                               |
|  |            | $x^2 + 20x + 25$ |                               |
|  |            | $x^2 + 21x + 1$  |                               |
|  |            | $x^2 + 22x + 1$  |                               |
|  |            | $x^2 + 23x + 5$  |                               |
|  |            | $x^2 + 24x + 5$  |                               |
|  |            | $x^2 + 24x + 25$ |                               |
|  |            | $x^2 + 27x + 1$  |                               |
|  |            | $x^2 + 27x + 5$  |                               |
|  |            | $x^2 + 29x + 5$  |                               |

| CODES GENERATED BY TRINOMIALS OF THE FORM $x^6 + ax^3 + b$ |            |   |                                 |
|--|------------|---|---------------------------------|
| $[q; n, 2t, d]$ -Code                                      | $\nu_2(u)$ | $h(x)$  | Weight enumerator               |
| $[31; 288, 6, 72]$   | 2          | $x^6 + 9x^3 + 25$<br>$x^6 + 14x^3 + 5$<br>$x^6 + 17x^3 + 5$<br>$x^6 + 22x^3 + 25$   | $(1 + 120z^{72} + 840z^{96})^3$ |
| $[31; 288, 6, 84]$   | 1          | $x^6 + x^3 + 5$<br>$x^6 + 6x^3 + 25$<br>$x^6 + 8x^3 + 25$<br>$x^6 + 9x^3 + 5$<br>$x^6 + 22x^3 + 5$<br>$x^6 + 23x^3 + 25$<br>$x^6 + 25x^3 + 25$<br>$x^6 + 30x^3 + 5$   | $(1 + 240z^{84} + 720z^{96})^3$ |
| $[31; 288, 6, 90]$   | 0          | $x^6 + 2x^3 + 5$<br>$x^6 + 4x^3 + 5$<br>$x^6 + 7x^3 + 5$<br>$x^6 + 7x^3 + 25$<br>$x^6 + 8x^3 + 5$<br>$x^6 + 11x^3 + 25$<br>$x^6 + 12x^3 + 25$<br>$x^6 + 14x^3 + 25$<br>$x^6 + 17x^3 + 25$<br>$x^6 + 19x^3 + 25$<br>$x^6 + 20x^3 + 25$<br>$x^6 + 23x^3 + 5$<br>$x^6 + 24x^3 + 5$<br>$x^6 + 24x^3 + 25$<br>$x^6 + 27x^3 + 5$<br>$x^6 + 29x^3 + 5$ | $(1 + 480z^{90} + 480z^{96})^3$ |

## REFERENCES

- [1] Brochero Martínez, F.E., Giraldo Vergara, C.R., Batista de Oliveira, L., *Explicit Factorization of  $x^n - 1 \in \mathbb{F}_q[x]$* , submitted for publication in Designs, Codes and Cryptography. Preprint available on <http://arxiv.org/abs/1404.6281>
- [2] Chen, B., Li, L., Tuerhong, R., *Explicit factorization of  $x^{2^m p^n} - 1$  over a finite field*. Finite fields and Their Applications **24** (2013) 95-104.
- [3] Ding, C., *The weight distribution of some irreducible cyclic codes* IEEE Trans. Inf. Theory **55** (2009) 955-960
- [4] Ding, C., Yang, J., *Hamming weights in irreducible cyclic codes*. Discrete Math. **313** (2013), 434-446.
- [5] Farrell, P. G., Castieira Moreira, J., *Essentials of Error-Control Coding* John Wiley & Sons Ltd (2006).
- [6] Golay, M. J. E., *Notes on Digital Coding*. Proc. IRE **37**, (1949) 657.
- [7] Lidl, R., Niederreiter, H. *Finite Fields*. Encyclopedia of Mathematics and Its Applications, Vol 20, Addison-Wesley 1983.
- [8] Fitzgerald R.W., Yucas J.L., *Explicit factorization of cyclotomic and Dickson polynomials over finite fields*. Arithmetic of Finite Fields. Lecture Notes in Computer Science, vol. 4547, pp. 1-10. Springer, Berlin (2007).
- [9] Meyn H., *Factorization of the cyclotomic polynomials  $x^{2^n} + 1$  over finite fields*. Finite Fields Appl. **2**, (1996) 439-442.
- [10] Sharma, A., Bakshi, G., *The weight distribution of some irreducible cyclic codes*. Finite Fields Appl. **18**, (2012) 144-159
- [11] Wang, L., Wang, Q., *On explicit factors of cyclotomic polynomials over finite fields*. Des. Codes Cryptogr. **63** (2012), no. 1, 87-104.

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDADE FEDERAL DE MINAS GERAIS, UFMG, BELO HORIZONTE, MG, 30123-970, BRAZIL,

E-mail address: [fbrocher@mat.ufmg.br](mailto:fbrocher@mat.ufmg.br)

E-mail address: [carmita@mat.ufmg.br](mailto:carmita@mat.ufmg.br)